Information Theory, Fall 2014	Iftach Haitner
Problem set 5	
January 7, 2015	Due: January 28

- Please submit the handout in class, or email the grader.
- Write clearly and shortly using sub-claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- It is allowed to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write his solution by *himself* (joint effort is only allowed in the “thinking phase")

1. Let $\pi = (\mathsf{P}, \mathsf{V})$ be a protocol with $\Pr\left[(\widetilde{\mathsf{P}}, \mathsf{V}) = 1\right] \leq \varepsilon$ for any s-size $\widetilde{\mathsf{P}}$, and for $k \in \mathbb{N}$ let $\pi^{(k)} = (\mathsf{P}^{(k)}, \mathsf{V}^{(k)})$ be the k-fold *sequential* repetition of π.[1] Prove that $\Pr\left[(\widetilde{\mathsf{P}^{(k)}}, \mathsf{V}^{(k)}) = 1^k\right] \leq \varepsilon^k$ for any $(s - kc_\pi)$-size $\widetilde{\mathsf{P}^{(k)}}$, where c_π is the communication size (i.e., number of bits sent) of π.

2. Let (E, D) be a perfectly correct encryption scheme for messages of length n and keys of length ℓ. Let $K \leftarrow \{0,1\}^\ell$. For each of the following cases find the best lower bound for ℓ.

   (a) $D(\mathsf{E}_K(m_0) || \mathsf{E}_K(m_1)) \leq \varepsilon$ for any $m_0, m_1 \in \{0,1\}^n$.

   (b) $\mathsf{SD}(\mathsf{E}_K(m_0), \mathsf{E}_K(m_1)) \leq \varepsilon$ for any $m_0, m_1 \in \{0,1\}^n$.

3. Let $f \colon \{0,1\}^n \mapsto \{0,1\}^n$ be (s, ε)-OWF, and let $\mathcal{H} = \{h \colon \{0,1\}^n \mapsto \{0,1\}^n\}$ be 2-universal family. Define g over $\{0,1\}^n \times \{0,1\}^n \times \mathcal{H} \times [n]$ by $g(x, r, h, i) = (f(x), r, h, h(x)_{1,\ldots,i}, b(x, r))$, for b being the Goldreich-Levin hardcore predicate (i.e., $b(x, r) = \langle x, r \rangle_2$). Find good as you can vales for s' and ε' such that $g(U_{2n}, H, I)$ has (s', ε')-entropy $H(g(U_{2n}, H, I)) + \frac{1}{2n}$, for $H \leftarrow \mathcal{H}$ and $I \leftarrow [n]$. You can assume that $\mathcal{H}$ is samplabe an evaluated by a size n algorithm.

[1] The parties interacts in k independent random sequential repetitions of π (i.e., the $i+1$ iteration stars after the i'th iteration ends), and $\mathsf{V}^{(k)}$ accepts if the verifiers accept in *all* k iterations.